公告本

申請日期：	89.7.4	案號：	89111919
類別：	G06F 12/14, G09C 1/00		

（以上各欄由本局填註）

發明專利說明書 480397

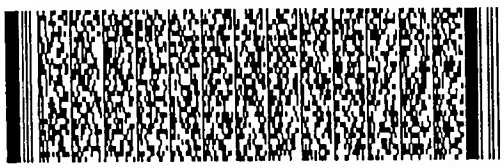
一、發明名稱	中文	安全記憶體
	英文	SECURE MEMORY
二、發明人	姓名（中文）	1. 李奧納德 J. 葛拉素
	姓名（英文）	1. LEONARD J. GALASSO
	國籍	1. 美國
	住、居所	1. 美國加州蘭卓聖塔瑪格麗特市泰普利托路21號
三、申請人	姓名（名稱）（中文）	1. 美商鳳凰工業股份有限公司
	姓名（名稱）（英文）	1. PHOENIX TECHNOLOGIES LTD.
	國籍	1. 美國
	住、居所（事務所）	1. 美國加州聖約瑟市東普朗利亞大道411號
	代表人姓名（中文）	1. 大衛 J. 鮑爾
	代表人姓名（英文）	1. DAVID J. POWER

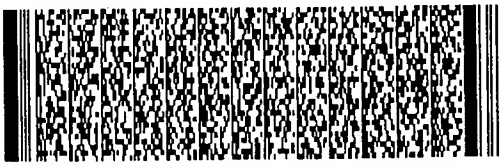
四、中文發明摘要　（發明之名稱：安全記憶體）

快閃記憶體經由禁能對裝置的寫入存取而安全化，如此防止未經授權更新或竄改內容。密碼引擎含括於快閃記憶體之一積體電路（IC）。試圖寫入快閃記憶體唯有於接收到的加密憑證由密碼引擎確認其真實性才能成功。若未確認其真實性，則外加至快閃記憶體的寫入致能信號線及電源皆被禁能。

英文發明摘要　（發明之名稱：SECURE MEMORY）

A flash memory is secured by disabling write access to the device, thereby preventing unauthorized updating or tampering of the contents. A cryptoengine is included in an integrated clircuit (IC) with the flash memory. An attempt to write to the flash memory is successful only if a received encrypted certificate is authenticated by the cryptoengine. If not authenticated, the write enable signal line and the power applied to the flash memory are





四、中文發明摘要　（發明之名稱：安全記憶體）

英文發明摘要　（發明之名稱：SECURE MEMORY）

disabled.

本案已向

國(地區)申請專利	申請日期	案號	主張優先權
美國 US	1999/06/18	09/335,704	有

有關微生物已寄存於　　寄存日期　　寄存號碼

無

五、發明說明（1）

發明背景

1. 發明領域

概略而言本發明係關於安全快閃記憶體儲存裝置，特別係關於一種使用加密確認真實性確保安全讀及寫存取至一快閃記憶體陣列之系統及方法。

2. 相關技術之說明

網際網路的出現以及不斷增加的電腦間互聯網路已經讓使用者可存取遠端大量資訊。同時也造成儲存於電腦記憶體的有價值的資料可由遠端使用者攻擊及訛用。例如具有中等複雜度的駭客可有效改變程式規劃快閃記憶體，該快閃記憶體可能儲存電腦的BIOS或前置啟動功能。為了解決此等攻擊，已經發展出多種加密系統及演算法來確保唯有經過授權的使用者才可更動儲存於記憶體的資料。

典型加密演算法例如RSA或DSA公鑰/密鑰加密要求使用者提出一數位憑證，一遠端使用者被授權由本地電腦的記憶體讀或寫之前，該數位憑證必須經過確認真實性。於遠端電腦、本地電腦或二電腦執行一程式通常可執行此種真實性確認。為了執行真實性確認，程式發送來回於遠端電腦與本地電腦間，或全部處理皆於其中一部電腦執行。

當真實性確認資訊在電腦間傳送時，真實性確認資訊被「駭客」所瞄準。即使僅於本地電腦執行真實性確認，於本地電腦執行的程式也產生外部活動，該外部活動也會被駭客瞄準。結果駭客可有效改變程式規劃記憶體，在處理中取消安全控制以及任何先前正在執行的基於軟體的安全

五、發明說明（2）

策略。因此加密以及真實性確認必須以可限制或免除駭客瞄準真實性確認資訊的方式進行因而確保記憶體資料不會被遠端訛用或攻擊而安全性。

發明概述

微處理器韌體之安全記憶體儲存裝置中，可使用密碼真實性確認而更新至一記憶體陣列。使用此種密碼真實性確認，試圖接取至記憶體陣列例如改寫記憶體內容例如「快閃更新」的軟體無法未有適當密碼憑據而獲得接取記憶體的程式規劃或記憶體的寫致能信號。

簡言之，與本發明符合一致，一種積體電路包含一記憶體用以接收包括至少一加密數位憑證的資料資訊，一致能信號其指示於記憶體進行操作，及一電源信號供給記憶體電源，一密碼引擎耦合至記憶體用以接收含括於資料資訊的加密數位憑證，確認接收的數位憑證的真實性，以及響應判定真實性而產生一安全信號，以及第一控制邏輯耦合至密碼引擎及記憶體用以響應安全信號選擇性耦合致能信號及電源信號中之至少一信號至記憶體，其中若未由密碼引擎產生安全信號，則致能信號及電源信號中之至少一者未耦合至記憶體。

本發明之又一特徵方面，一種保全一記憶體之安全之方法，包括一記憶體及一密碼引擎且係於一積體電路上實施，包含下列步驟：於記憶體接收資料資訊，該資料資訊包括至少一加密數位憑證、一致能信號其致能於記憶體操作及一電源信號其供給記憶體電源；一密碼引擎證實接收

五、發明說明（3）

到的數位憑證的真實性；響應判定真實性產生一安全信號；以及響應安全信號選擇性耦合至致能信號及電源信號之至少一者至記憶體，其中若未產生安全信號，則致能信號及電源信號中之至少一者未耦合至記憶體。

圖式之簡單說明

圖1為根據本發明之安全快閃記憶體之方塊圖。

圖2為根據本發明之安全更新快閃記憶體之處理之流程圖。

圖3為根據本發明於一安全快閃記憶體確認真實性處理之方塊圖。

較佳具體實施例之詳細說明

本發明將於特定實施例之內容說明，但本發明絕非意圖囿限於此。

根據本發明之安全快閃記憶體中，嵌置的密碼引擎可用來證實基於軟體的以作業系統為主的密碼引擎的真實性。經由耦合確認真實性能力至支援安全快閃記憶體的平臺，信任鏈直接移動至系統積分器及/或直接設備製造商（OEM）的掌控，其更可處理快閃記憶體組件的更新。密碼引擎（及其微碼）於快閃記憶體陣列整合可於極高速電路（VHSIC）硬體描述語言（VHDL）層面進行，當如此整合時可共用同一積體電路（IC）外殼。

圖1為根據本發明之安全快閃記憶體100之方塊圖。如圖1所示，安全快閃記憶體100包括快閃記憶體陣列10，密碼引擎20、第一開關40及一第二開關控制50。快閃記憶體10

五、發明說明 (4)

及密碼引擎20接收位址線及資料線。位址線及資料線的數目可改變且隨安全快閃記憶體100實施的特定系統而定。圖1中位址線表示為32位元而資料線示為8、16或32位元。

可用於執行本發明之VHDL密碼引擎係由Greg Kazmierczak等人，第5,764,762號專利案，專利名稱「內容計量系統」揭示。此種內容計量系統係採用Keith Klemba等人，第5,651,068號專利案，發明名稱「國際密碼架構」。二案皆併述於此以供參考。

密碼引擎20包括密碼引擎控制邏輯22、韌體24、RAM26、ROM28及處理器或CPU 30。密碼引擎控制邏輯22例如可由邏輯電路聚集體形成，邏輯電路例如邏輯閘、算數邏輯單元(ALUS)及其他業界人士已知的電路。密碼引擎控制邏輯22可於VHDL具體表現且插入任何特殊應用積體電路(ASIC)核心內部。密碼引擎控制邏輯22可執行業界人士已知的業界標準密碼演算法例如Triple DES、RSA及DSA。當試圖寫至已經被證實真實性的快閃記憶體陣列10時，由密碼引擎控制邏輯22與安全線60產生安全信號。

韌體24儲存由CPU 30執行的微指令集合，指示密碼引擎控制邏輯22進行解密及確認真實性，且可實施作為非揮發性儲存裝置例如NVRAM、ROM、PROM或EPROM。韌體24的微指令形成一程式使用公鑰演算法例如DSA具體表現例如基於鑰的密碼系統。ROM 28為密鑰儲存裝置可接取密碼引擎控制邏輯22，但無法由密碼引擎20外側存取。ROM 28對執行安全快閃記憶體100之電腦系統儲存一獨特的數位憑

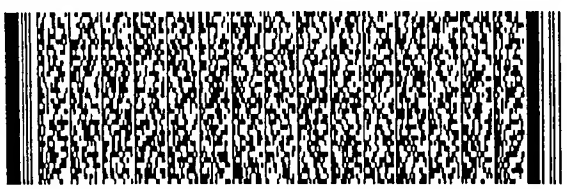
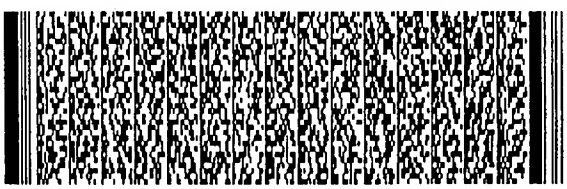
五、發明說明 (5)

證。此數位憑證較佳於安全快閃記憶體100製造時置於ROM 28。若韌體24之微指令具體表現一執行公鑰演算法如DSA之程式，則此數位憑證表示公鑰/密鑰對的密鑰。

雖然韌體24及ROM 28於圖1顯示為分開元件，但須瞭解二者可具體表現於同一非揮發性儲存裝置。結果儲存於韌體24的微碼也無法由密碼引擎20外側存取。

快閃記憶體陣列10較佳為非揮發性記憶體儲存裝置例如PROM、EPROM或EEPROM。其可儲存執行安全快閃記憶體100之電腦系統使用的資料及資訊。例如快閃記憶體陣列10可儲存電腦系統使用的BIOS或其他前置啟動資訊來啟動其作業系統。快閃記憶體陣列100的大小可改變，但通常可為二的某種倍數例如8百萬位元。

如圖1所示，快閃記憶體陣列通常配置有電源線VPP 70、資料線15、位址線25、寫致能線80以及其他可拉到連接接腳的線(圖中未顯示)。寫致能線80路由通過第二開關控制50，VPP線70路由通過第一開關控制40。二開關控制根據安全信號線60係由密碼引擎控制邏輯22控制。第二開關控制50例如可執行為一AND閘，該閘於一輸入端接收原先寫入致能信號，及於另一輸入端接收來自密碼引擎控制邏輯22輸出的安全信號。VPP信號路由通過其中的第一開關控制40例如可實施為電源MOSFET，作為飽和開關其可供應快閃記憶體陣列10於程式規劃期間的電流驅動需求。除非密碼引擎控制邏輯22產生/主張安全信號，否則寫入致能線80及VPP線70的信號不會被閘控至快閃記憶體陣列

五、發明說明 (6)

10。結果快閃記憶體陣列10無法未經主張安全信號而被改變程式規劃亦即被寫入。

密碼引擎控制邏輯22唯有於進行適當真實性確認時，才透過資料匯流排及控制協定響應適當數位憑證的提出而產生安全信號。經由適當提出數位憑證，寫入致能線80及VPP線70被主動化，因而有效對使用者呈現正常快閃記憶體陣列10。若未呈現此種憑證亦即呈現訛誤的憑證，則寫入致能信號及VPP信號至快閃記憶體陣列10的閘控動作不會發生，如此避免快閃記憶體陣列10的內容改變。

如此形成一種鎖定快閃記憶體陣列，其內容唯有於執行適當憑證時才可被解除鎖定。此外除了密碼引擎20本身外，於平臺上無須任何微處理器或其他運算實體的運作。結果由供電瞬間開始以及在控制實體系統BIOS或韌體有機會開始執行之前可確保控制實體的安全。經由適當鎖定快閃記憶體陣列10的內容，唯有於軟體已經提出適當憑證，憑證提出給安全快閃記憶體100且證實憑證的真實性才可進行更新。

因真實性的確認係在快閃記憶體陣列10及密碼引擎20外殼內部進行，因此並無任何可被駭客所「瞄準」的外部活動。如此安全快閃記憶體100極為安全。

圖2為根據本發明之快閃記憶體之操作方塊圖。於正常操作下，快閃記憶體陣列10類似標準快閃ROM被供電、致能及定址。但若快閃記憶體陣列被寫入因而目前的內容被新內容替代時，正常作業被變更。首先，控制實體之欲改

五、發明說明 (7)

變程式規劃安全快閃記憶體100的快閃記憶體陣列10之程式或系統藉由嘗試寫入作業而定址快閃記憶體陣列10(步驟205)。需瞭解雖然此項程式係就寫入作業而言，但基本處理同等適用於其他作業例如讀取。然後定址快閃記憶體陣列10的程式形成一加密憑證，該憑證係對應於加密寫入作業(步驟210)。為了形成加密憑證，寫入作業內容可使用控制實體的公鑰/私鑰對之公鑰簽章。加密後的數位憑證供給或傳輸給安全快閃記憶體100(步驟215)。如圖2所示，各步驟需於安全快閃記憶體100外部執行。後文討論之所有隨後步驟皆係於快閃記憶體100內部執行。

於傳輸加密數位憑證後，憑證由安全快閃記憶體100接收(步驟220)。密碼引擎20使用儲存於韌體24的加密演算法來解密接收到的加密憑證(步驟225)。例如若憑證已經使用控制實體公鑰加密，則可以密鑰解密，密鑰可儲存於ROM 28。一旦憑證被解密，密碼引擎20證實解密的憑證或確認其真實性(步驟230)。真實性確認可由密碼引擎控制邏輯22決定解密資訊是否為相干性執行。例如程式規劃操作的格式或語言包括若干可由密碼引擎控制邏輯22確認的位元圖樣來決定解密資訊是否真實。

圖3為根據本發明之安全快閃記憶體中真實性確認處理之方塊圖。當資料外加至位址線及資料線時，此等線被監視是否有任何指令存取快閃記憶體陣列10的一個位置。例如此等線被監視資料位元組(步驟305)。然後位元組被集合成為封包(步驟310)。集合例如可使用簡單協定基於位

元流的字元定界標及檢查和進行。若封包無效例如若在某一段字元無法找到定界標，則真實性確認處理返回步驟305。

若封包有效，則密碼引擎20試圖以前述步驟225之相同方式解密封包(步驟315)。若被解密的封包係使用對應公鑰加密或使用真實憑證簽章，則封包被解密時具有相干性，例如若封包類似含功能碼以及若干額外參數的標準化封包則封包為相干性。若封包為非相干性，則封包被忽略，快閃記憶體陣列10保持安全，真實性確認處理返回步驟305。

若封包為相干性，則封包被語法剖析而解碼含於封包的指令(步驟320)。若指令為無效則處理再度返回步驟305。但若指令為有效則執行指令(步驟325)。被執行的指令例如致能存取快閃記憶體陣列10(步驟330)。另外，被執行的指令可為禁能存取至快閃記憶體陣列10(步驟335)。當快閃記憶體陣列10被致能時，如業界已知，使用標準快閃記憶體陣列10程式規劃協定重新程式規劃。

回頭參考圖2，若對應解密寫入作業的解密憑證被證實真實性，例如由圖3的處理證實真實性，則密碼引擎控制邏輯22於安全線60上產生信號(步驟235)。主張安全線60致能寫入致能線80上寫入致能信號透過第二開關控制50與安全寫入致能線85而被閘控至快閃記憶體陣列10(步驟240)。此外，第一開關控制40允許經由安全電源線VPP線75響應安全線60的主張而允許電源信號VPP進入快閃記憶

五、發明說明 (9)

體陣列10(步驟245)。使用安全電源線VPP及安全寫入致能信號閘控至快閃記憶體陣列10，快閃記憶體陣列10的內容係根據解密後的寫入操作更新(步驟250)。特別解密後寫入作業係作為提供於位址線及資料線上的資料而呈現給快閃記憶體陣列10。

但若解密後的憑證未由密碼引擎控制邏輯22證實真實性，則密碼引擎控制邏輯22未主張信號與安全線60(步驟255)。結果第一開關邏輯40封阻電源信號VPP的閘控至快閃記憶體陣列10(步驟260)，第二開關邏輯50封阻寫入致能信號的被閘控至快閃記憶體陣列10(步驟265)。若無電源信號VPP及寫入致能信號閘控至快閃記憶體陣列10，則快閃記憶體陣列10的內容無法被更新(步驟270)。

雖然具體實施例特別目標鎖定快閃記憶體裝置，但該技術也自適應於其他記憶體物件或其他記憶體電路例如I/O線、電子信號、I/O晶片的暫存器排組或特定平臺上的埠。此外雖然本具體實施例係針對寫入作業的保護，但須瞭解該技術也自適應於阻止任何類型未經授權的動作例如讀取或執行指令。

前文本發明之較佳具體例之說明係供舉例說明之用。絕非意圖羅列盡淨或限制本發明於揭示的精確形式。鑑於前文教示且由本發明之實施可取得多種修改及變更。選擇及說明此等具體實施例係供解釋本發明的原理以及實際應用來使業界人士可利用本發明於多種不同具體實施例以及適合特定預期用途的多種修改。本發明之範圍係由隨附之申

五、發明說明（10）

請專利範圍及其相當範圍所界定。

六、申請專利範圍

1. 一種積體電路，包含：

一記憶體用以接收資料資訊，包括至少一加密數位憑證，一致能信號其致能於記憶體上執行的作業，及一電源信號其對記憶體供給電源；

一密碼引擎，密碼引擎耦合至記憶體用以接收含括於資料資訊的加密數位憑證確認接收得的數位憑證之真實性，以及響應決定真實性而產生一安全信號；以及

第一控制邏輯，第一控制邏輯耦合至密碼引擎及記憶體用以響應安全信號，選擇性耦合致能信號及電源信號之至少一者至記憶體，

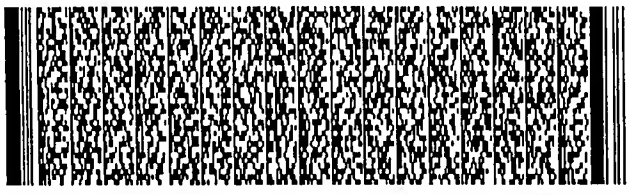
其中若未由密碼引擎產生安全信號，則致能信號及電源信號中之至少一者為耦合至記憶體。

2. 如申請專利範圍第1項之積體電路，其中第一控制邏輯包括一邏輯閘，其接收安全信號及致能信號，以及響應安全信號耦合致能信號至記憶體。

3. 如申請專利範圍第1項之積體電路，其中第一控制邏輯包括一電晶體用以響應安全信號，選擇性耦合電源信號至快閃記憶體。

4. 如申請專利範圍第1項之積體電路，其中第一控制邏輯包括一邏輯閘，其接收安全信號及致能信號，以及響應安全信號而耦合致能信號至記憶體，以及包括一電晶體用以響應安全信號而選擇性耦合電源信號至記憶體。

5. 如申請專利範圍第1項之積體電路，其中密碼引擎包括ROM用以儲存用於確認加密數位憑證之真實性的一本地



六、申請專利範圍

數位憑證。

6. 如申請專利範圍第5項之積體電路，其中密碼引擎進一步包括第二控制邏輯，用以使用本地數位憑證解密且確認接收得的數位憑證真實性。

7. 如申請專利範圍第6項之積體電路，其中密碼引擎進一步包括第三控制邏輯，用以於確認接收得的數位憑證之真實性時產生安全信號。

8. 如申請專利範圍第1項之積體電路，進一步包含非揮發性記憶體，耦合密碼引擎，用以儲存由密碼引擎使用的微指令而確認接收得的數位憑證之真實性。

9. 如申請專利範圍第8項之積體電路，進一步包含一處理器耦合至密碼引擎，用以執行儲存於非揮發性之記憶體之微指令，以及基於執行的微指令，指示密碼引擎確認接收得的數位憑證之真實性。

10. 如申請專利範圍第1項之積體電路，其中記憶體為一快閃記憶體陣列。

11. 一種保全一記憶體之安全性之方法，包括一記憶體及一密碼引擎且係於一積體電路上執行，該方法包含下列步驟：

於記憶體接收資料資訊，資料資訊包括至少一加密數位憑證，一致能信號其致能於記憶體上執行的作業，及一電源信號其對記憶體供給電源；

於密碼引擎確認接收得的數位憑證之真實性；

響應真實性的確定產生一安全信號；以及

六、申請專利範圍

響應安全信號，選擇性耦合致能信號及電源信號中之至少一者至記憶體，

其中若未由密碼引擎產生安全信號，則致能信號及電源信號中之至少一者為耦合至記憶體。

12. 如申請專利範圍第11項之方法，其中選擇性耦合步驟包括響應安全信號而耦合致能信號及電源信號至記憶體之子步驟。

13. 如申請專利範圍第11項之方法，其中確認真實性步驟包括儲存一本地數位憑證於一ROM，該ROM可由密碼引擎存取而確認被加密的數位憑證真實性之子步驟。

14. 如申請專利範圍第13項之方法，其中確認真實性步驟進一步包括使用本地數位憑證且確認接收得的數位憑證真實性之子步驟。

15. 如申請專利範圍第14項之方法，其中產生步驟包括當接收得的數位憑證的真實性經過確認時產生安全信號之子步驟。

16. 如申請專利範圍第11項之方法，進一步包括儲存微指令於記憶體之非揮發性記憶體，該微指令由密碼引擎用以確認接收得的數位憑證之真實性之步驟。

17. 如申請專利範圍第16項之方法，進一步包含執行儲存於非揮發性記憶體之微指令之步驟，以及基於被執行的微指令指示密碼引擎確認接收得的數位憑證之真實性之步驟。

89111919

圖式

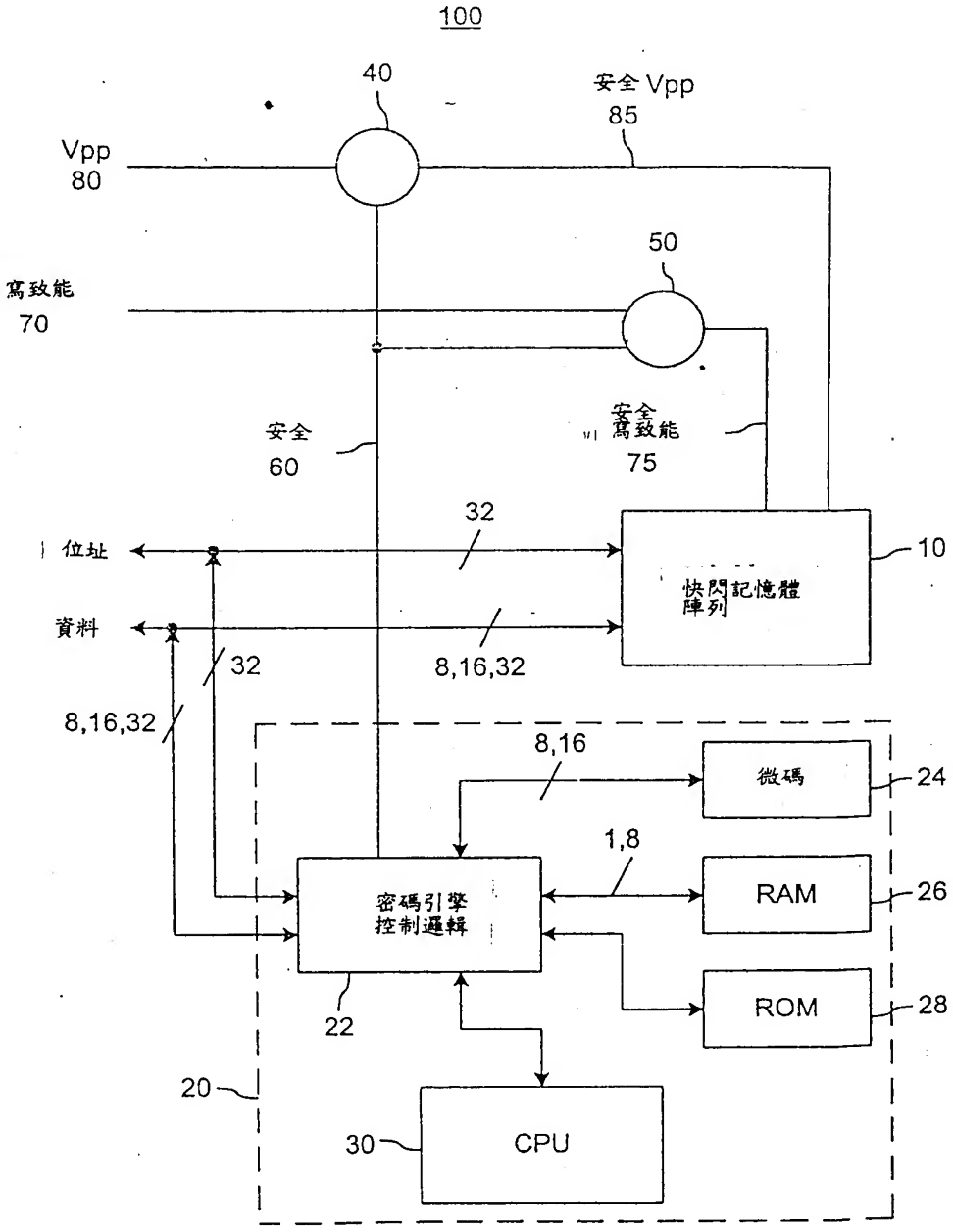


圖 1

圖式

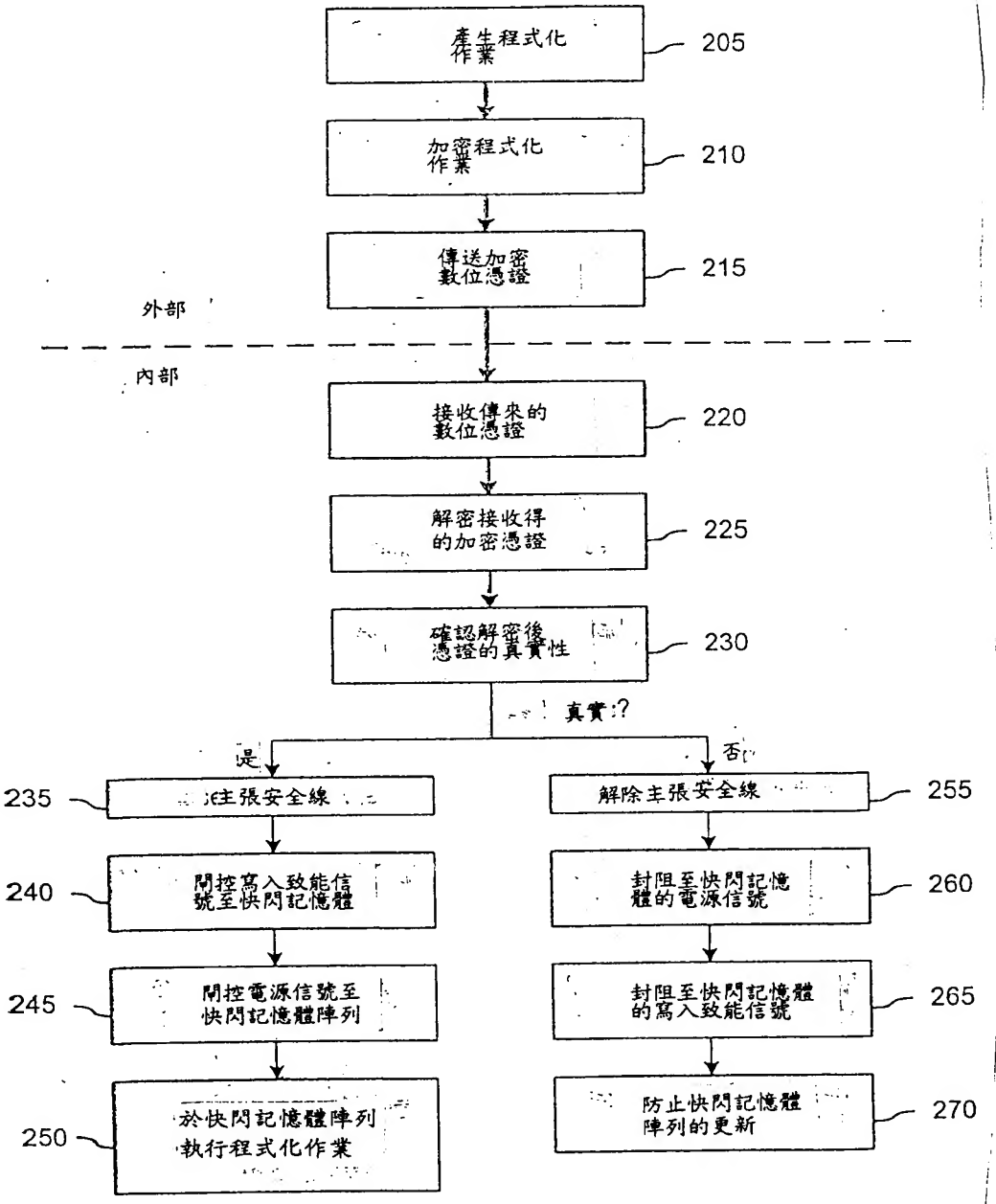

產生程式化作業
205
加密程式化作業
210
傳送加密數位憑證
215
外部
內部
接收傳來的數位憑證
220
解密接收得的加密憑證
225
確認解密後憑證的真實性
230
真實?
是
否
235
主張安全線
解除主張安全線
255
開控寫入致能信號至快閃記憶體
240
封阻至快閃記憶體的電源信號
260
開控電源信號至快閃記憶體陣列
245
封阻至快閃記憶體的寫入致能信號
265
於快閃記憶體陣列執行程式化作業
250
防止快閃記憶體陣列的更新
270

圖 2

圖式

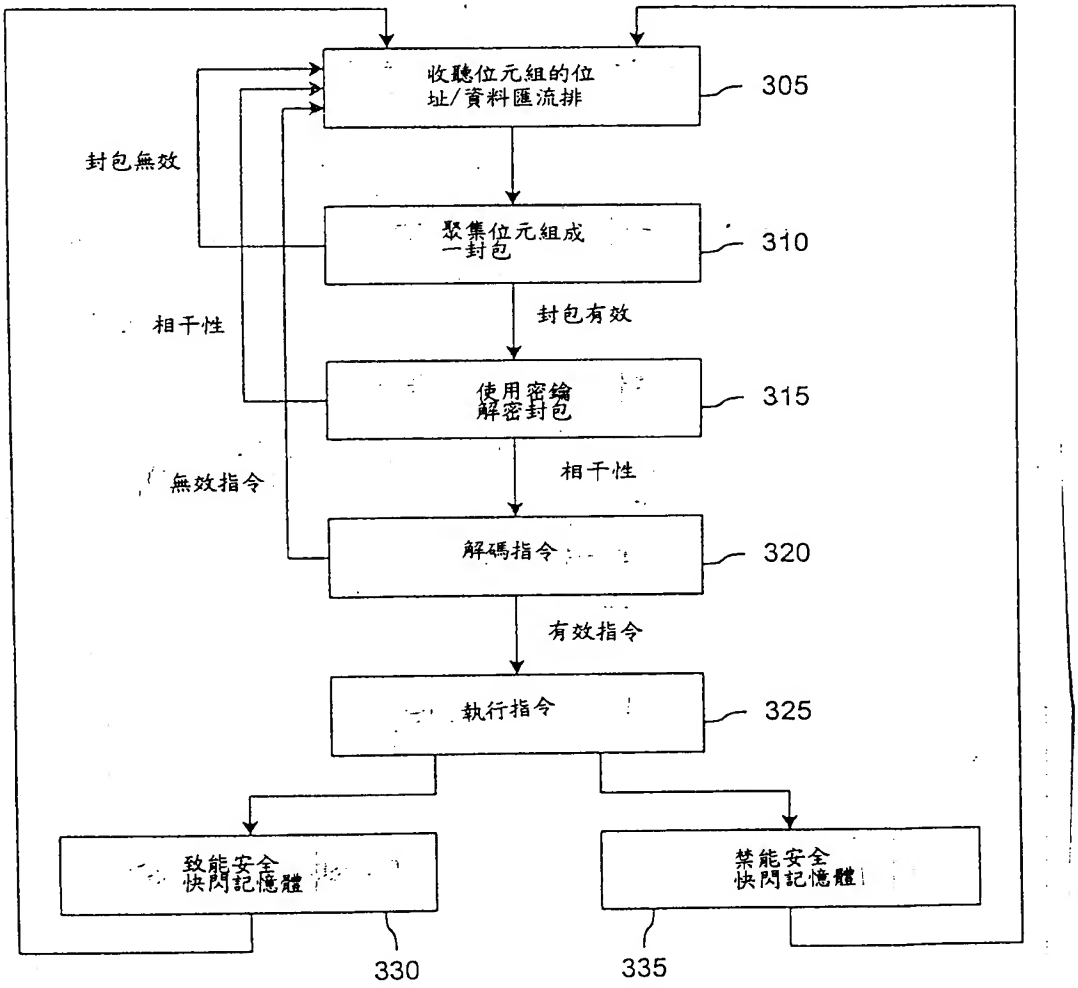

收聽位元組的位址/資料匯流排
305
封包無效
聚集位元組成一封包
310
封包有效
相干性
使用密鑰解密封包
315
相干性
無效指令
解碼指令
320
有效指令
執行指令
325
致能安全快閃記憶體
禁能安全快閃記憶體
330
335

圖 3